はじめての情報通信技術と情報セキュリティ　諏訪敬祐・関良明

本書は文系・理系の１～2 年生が大学講義の教科書として使用することを想定。

トラヒック

電子的におこなわれている
　「文書の電子化の促進に向けて– - 経済産業省」という使い方と同じようだ。若い人は使わないだろう。

＝＝＝Web＝＝＝
用語「トラヒック」は主に電話系で使われている。 通信系ではもっぱらトラフィックと呼ばれるが、表現が異なるだけで同義である。

トラヒック
【英】: traffic
通信において接続される単位，すなわち，通話や一連のデータの通信等をトラヒックと呼び，交通と区別するとき，特に「通信トラヒック(teletraffic)」と呼んでいる．電話網を例にとると，交換接続の要求である電話呼が時々刻々到着し，ある時間，回線などを保留して接続処理や通話の終了とともに退去していく．電話呼の到着，回線保留時間，通話相手などは時間的・空間的に変動しており，それらを総称してトラヒックと呼んでいる．
＝＝＝＝＝＝＝＝＝　＝＝＝＝＝＝＝＝＝　＝＝＝＝＝＝＝＝

電話音声などのアナログ信号の情報をディジタル情報に変換する過程を図 2．16 に示す．ディジタル化は入力［アナログ信号（情報)］→**標本化→量子化→符号化**→出力［ディジタル信号（情報)］という順序で行われる．標本化は連続した波形のアナログ信号を一一定周期で分割することである．標本化をサンプリングとよぶ場合もある．量子化は標本化波形の振幅を離散的な数値に変換することである．また，符号化は離散的な数値を 2 進数へ変換することである．

ナイキスト
（Nyquist）の標本化定理として人力信号の最高周波数 f_m が B に制限されているとき，標本化周波数 f s が f s＞2 B の条件を満たす場合，標本化された波形よりもとの信号を再生することができることが知られている．具体的には，アナログ信号に含まれる最高周波数の 2 倍以上の標本化周波数でサンプリングすればよい．**電話では，最高周波数は 3.4kHz** であるが，実際には余裕をみて 4kHz とし，標本化周波数は 8kHz としている．このとき，標本化周期 T は 1／8000（s）＝125／μs である．高音質の音声を記録する CD の場合，高音域の信号成分を含むため最高周波数は約 20kHz であるので，標本化周波数は 44.1kHz となっている．**高品質ディジタル電話の標本化周波数は 16kHz** である．また，音声の量子化ビット数は図 2.18 に示すように通常品質では 8bit（2^8＝256 段階：256 個の離散的な振幅値に量子化)，高品質では 16bit（2^{16}＝65,536 段階）である．
　ディジタル信号をネットワークで伝送するときの速度を伝送速度とよび，1 秒間に何ビット送信したかで数値で表現する．単位はビット／秒である．bit/s, bps などで表す．電話の伝送速度は標本化周波数が 8kHz，1 標本値について 8bit で符号化されるので，8kHz×8bit＝64kbit/s となる．

2）文字コードを用いた文字表現
　コンピュータでは文字（漢字，数字，ひらがななど）の形では処理できない．文字はコード化（1，0 で表現）が行われる．アルファベット，数字，記号は 1byte＝8bit（256 通り）で表現され，漢字は 2byte＝16bit（65，536 通り）で表現される．これらの文字は表 2.2 に示す各種文字コードで表現される．ASCII コードは英数字，記号文字，制御コードを表す 7 ビットコードであり，JIS 漢字コードは英数字，記号文字，ひらがな，カタカナ，漢字を表す 16 ビッ

トコードである．図 2.19 に JIS 漢字コードの文字コード表の読み方を示す．ひらがなの「あ」の場合は横の列 4 番目の第 1 バイト 00100100＝24 と縦の列 2 番目の第 2 バイト 00100010＝22 から 16 進文字コードで「2422」のように表現される．

表 2.2　文字コードの種類

サイズ	コード名称	概　要
1 byte	ASCII コード	英数字，記号文字，制御コードを表す 7 ビットコード
	JIS コード	ISO コード（国際規格）をもとにした半角文字コード（JIS X0201）
	EBCDIC コード（拡張 2 進化 10 進コード）	汎用コンピュータの標準である 8 ビットコード
2 byte	JIS 漢字コード	英数字，記号文字，ひらがな，カタカナ，漢字を表す 16 ビットコード
	シフト JIS コード	JIS 漢字コードの表現領域をずらした 16 ビットコード
	Unicode	世界中の文字を 2 byte で表す国際規格の 16 ビットコード
マルチバイト	日本語 EUC コード	UNIX で使用される 1～3 byte のマルチバイトコード

コンピュータの演算処理は当初，複数の半導体チップが連携して行っており，この半導体チップ群を CPU とよんでいた．中央処理装置を 1 個の半導体チップに集積した部品がマイクロプロセッサである．現在のコンピュータではマイクロプロセッサですべての演算を行い，プログラムの読込み，実行を行っている．マイクロプロセッサには，1 回の命令で同時に処理できるデータ量によって **16bit，32bit，64bit などの種類があり，一般に bit 数値が大きいものほど性能が高い**．また，CPU の演算速度は CPU クロック周波数が高いはど逆性が速く，クロック周波数 3．2GHz の CPU の演算速度は 1／3.2GHz＝0.3125 ns ＝0.3125×10^{-9} s である．

ハードディスクのデータは，磁気ディスクを同心円状に**シリンダ**，回転方向に**セクタ**とよばれる微小領域に分割して記録される．セクタの円周上の集合を**トラック**とよぶ．ハードディスクでは，複数枚の磁気ディスクが同じ回転軸に取り付けられ，アクセスアームの先端の磁気ヘッドが移倒しながらトラックの記憶面にアクセスする．複数のアクセスアームはすべて同時に動くため 1 回に複数の磁気ディスクからデータを読取り，書込みできるので同じ距離にあるトラックの集合を一つにまとめてシリンダとよぶ．この場合，ハードディスクの記憶容量は以下の式で求められる．

記憶容量＝1 セクタあたりの記憶容量×1 トラックのセクタ数×1 シリンダあたりのトラック数×シリンダ数　　(2・1)

たとえば，シリンダ数＝1800 シリンダ，1 シリンダあたりのトラック数＝40 トラック，1 トラックのセクタ数＝64 セクタ，1 セクタあたりの記憶容量＝600byte とすると，このハードディスクの記憶容量は以下のようになる・

記憶容量＝600×64×40×1800byte
＝2764800000byte
＝2764800000÷1024÷1024÷1024GB
≒2.57GB

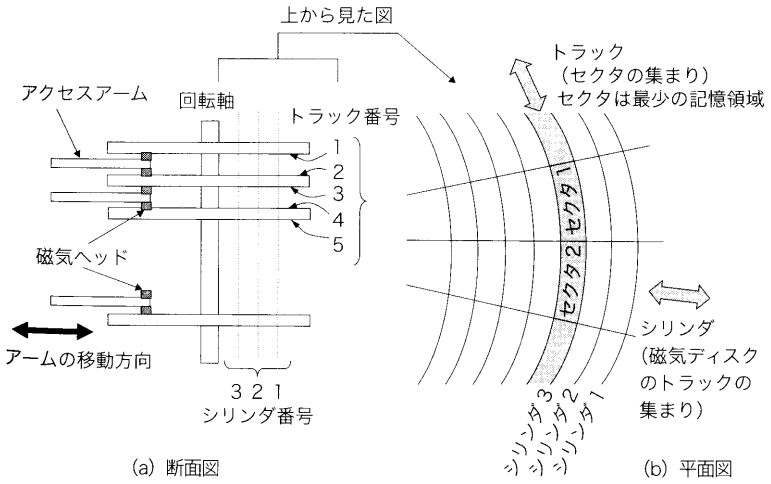


図 3.16　ハードディスクの仕組み

DVD（Digital Versatile Disk）は図 3・18 のように大きさは CD と同じ直径 12cm，厚さ 1.2mm（片面 0.6mm×2）であるが記憶容量は 4.7GB～17GB と大容量である．DVD は 0・6mm のディスクを 2 枚貼り合わせた構造であり，**レーザの焦点をずらすことにより 2 層の記録層への書込みを可能としている**．

CD－RW（Rewritable）は図 3．20 のように記録層（銀，インジウム，アンチモンなどの相変化金属）の結晶状態をレーザ光線により結晶状態，非結晶状態（アモルファス状態）に相変化の制御を行って書込み，消去を行う．データの記録の書換え速度は最大 10 倍速，書換え回数は約 1,000 回程度である．図 3.21 のように記録のときは出力の強いレーザ光線を照射して休息加熱，冷却を行い，**アモルファス状態でデータを書き込む**．消去のときは出力の弱いレーザ光線を照射してゆっくり冷却し，**結晶状態をつくり出してデータの消去**を行う．

機械語，アセンブリ言語のような低級言語（低水準言語）
・・・低級言語（低水準言語）という言い方は適切ではない。

現在は，CCD より低電圧回路で構成できるため消費電力が小さく，読み出し速度が高速な CMOS（Complementary Metal Oxide Semiconductor：相補型 MOS）撮像素子がディジタルカメラ，スマートフォンで主に使用されている．一つ一つの画素に ON／OFF スイッチ回路を組み込むことで蓄積された電荷をその場で電圧に変換するので処理速度が速い．

液晶の主な種類を表 4.3 に示す．当初の液晶はモノクロ（白黒）の TN 液晶であったが，カラー化の需要にともない，TSTN 液晶が用いられている液晶ディスプレイに配置した電極に電圧をかけて駆動する代表的な方式としては図 4.21 に示すように単純マトリックス方式と**アクティブマトリックス方式**の二つがある．単純マトリックス方式は，電卓，ワープロ，パソコンなど，主に静止画用に幅広く使用されている．アクティブマトリックス方式は，テレビなどの高い画質と速い応答速度が要求される動画の表示に使われている．

駆動の原理は単純マトリックス方式の場合，電流を導く「導線」を格子上にはりめぐらせ，縦横それぞれのタイミングをあわせて電気信号を送ると，縦横の交差する場所の画素が点灯する．縦横の導線の組合せで目的とする複数の画

素を同時に点灯できる．アクティブマトリックス方式は，単純マトリックス方式の構造に加えて，画素の一つ一つに「**アクティブ素子**（トランジスタ回路」を付加したものである．アクティブ素子により目的の画素を確実に点灯させたり消したりすることができる．

・・・液晶は難しい。

OSl 参照モデル

プロトコルの階層化に際しては，層の数と各層にもたせるべき機能を明らかにする必要がある．このため国際標準化機構（ISO）が 1983 年に制定したプロトコルの階層とその機能に関する標準が，開放型システム間相互接続基本参照モデル（OSI：Open Systems Interconnection Basic Reference Model）であり，通称「OSI 参照モデル」とよばれる．OSI 参照モデルはネットワークアーキテクチャの標準を規定したものである．OSI 参照モデルはプロトコルそのものを規定したものではなく，個別のプロトコルを決める際の全体的な枠組みを示している．今日では，国際的な標準化機関やフォーラム，コンソーシアムでプロトコルを検討する場合の土台の役割を果たしている．

OSI 参照モデルは図 5．9 のように 7 階層（7 レイヤ）から構成される．同一層間の規定をプロトコル，階層間の規定をインタフェースとよぶ．OSI 参照モデルでは，エンドのコンピュータ（エンドシステム）と中継を行うコンピュー（中継システム）の 2 種類があり，中継システムは下位の 3 階層のみの機能を有する．各層の名称と機能概要を上位層から順に以下に述べる．

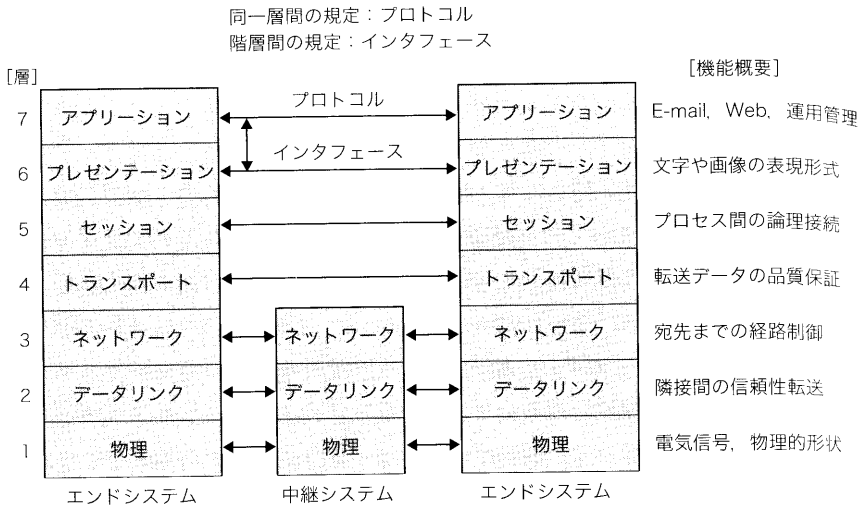


図 5.9　OSI 参照モデル（7 階層）

(1) ドメイン名とDNSサーバ

インターネット上の住所である IP アドレスは 5.4 節で述べたように 10 進数で表現するが，人間にとっては非常に扱いにくい．そこで IP アドレスとは別に，人間が記憶しやすい名前を設けて利用する．この名前のことをドメイン名（domain name）という．ドメイン名はドットで区切られて階層化されており，第 1 階層は国際的に一意に割り当てられた国名を示し，第 2 階隣以上は各国の管理機関で管理される．

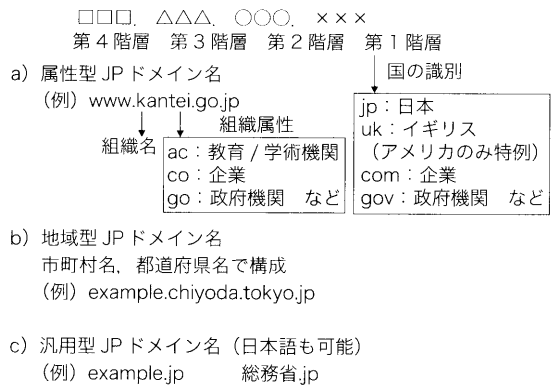


図 5.24　ドメイン名と構造

人間にとって便利なドメイン名であるがルータには理解できず，パケットを宛先まで届けることができないので，**ドメイン名から IP アドレスに変換**する仕組みが必要となる．この変換を行う機構が **DNS**（Domain Name System）であり，この変換サービスを提供するコンピュータのことを DNS サーバ（またはネームサーバ）という．相手と通信したいクライアント側のコンピュータプログラム（リゾルバ）は，図 5.25 に示すように DNS サーバに通信相手のドメイン名を送ってその IP アドレスを教えてもらい，その後にこの IP アドレスにより通信相手にアクセスすることになる．**リゾルバ**とはネームサーバにホスト名を通知して IP アドレスの検索を依頼したり，その道を依頼したりするクライアント側のプログラムである．DNS サーバとリゾルバとのやりとりのためのプロトコルが **DNS プロトコル**であり，トランスポート層のプロトコルは **UDP** を用いる．DNS サーバは各ネットワークに設置されるが，世界中のドメイン名と IP アドレスの対応情報を保持しているわけではなく，図 5.26 に示すように DNS サーバは階層化されている．各階層のドメイン名に対応した DNS サーバがあり，配下の DNS サーバのドメイン名と IP アドレスを管理している．リゾルバからの問合せに対して，自 DNS サーバ（ローカル DNS）の範囲外の場合には，上位階層の DNS サーバへ問い合せる．DNS サーバでは検索結果を一時的に記憶（キャッシュ）しておき，検索の効率化を図っている．なお，最上位の DNS サーバはルート DNS サーバといい，全世界に 13 個設置れている．このように **DNS サーバは**，インターネットの非常に重要な**電話帳の役割**を果たしている．

映画などの動画ファイルをサーバからクライアントのコンピュータへダウンロードしながら，再生する技術を**ストリーミング**という．

CDMA（Code Division Multiple Access）：符号分割多元接続．ユーザごとに異なる符号を割り当てて通信を行う．

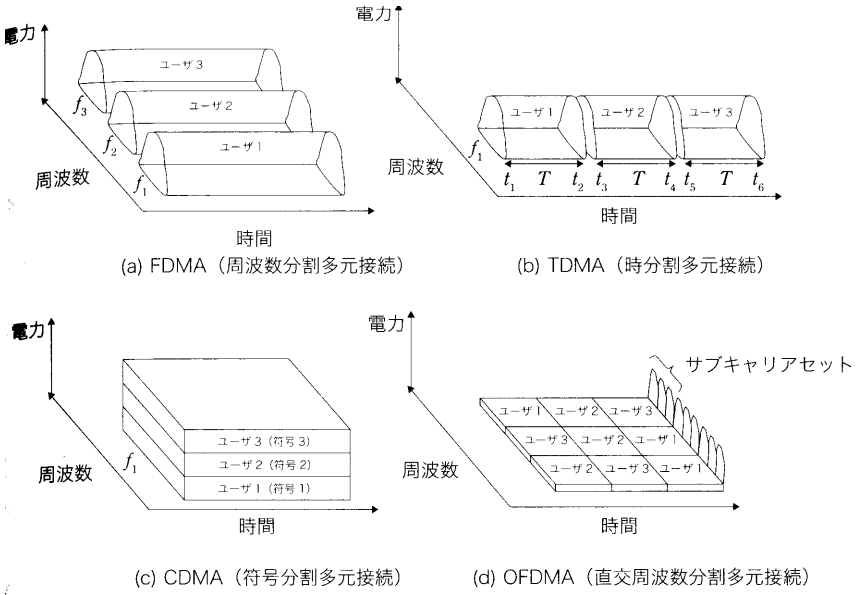


図 6.3　さまざまなアクセス方式

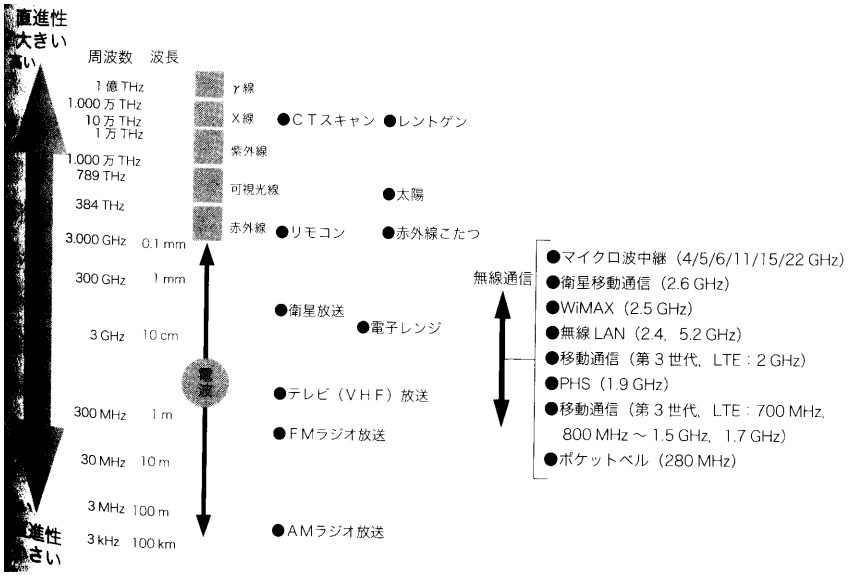
表 6.2　無線 LAN の規格

方式名称	802.11a	802.11b	802.11g	802.11n	802.11ac
最大伝送速度	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s	6.9 Gbit/s
標準化時期	1999 年	1999 年	2003 年	2009 年	2014 年
周波数帯	5 GHz 帯	2.4 GHz 帯	2.4 GHz 帯	2.4/5 GHz 帯	5 GHz 帯
多重化方式，変調方式	OFDM	DSSS/CCK	OFDM	OFDM/MIMO	OFDM/MIMO

CCK：Complementary Code Keying（相補符号変調）
DSSS：Direct Sequence Spread Spectrum（直接スペクトラム拡散方式）
MIMO：Multiple Input Multiple Output
OFDM：Orthogonal Frequency Division Multiplexing（直交周波数分割多重）

11ac は MIMO のアンテナ数を 11n の 2 倍とし，多値変調方式を適用して大幅な高速化を実現している．

アクセスポイントについては，世界の機器ベンダーが製造したものについて相互接続性を保証するために WECA（Wireless Ethernet Compatibility Alliance）という業界団体が相互接続を検証した製品に国際規格の認定品であることを示す Wi－Fi（Wireless　Fidelity）のロゴが貼付されている．このため**無線 LAN は Wi－Fi ともよばれる**．



直進性

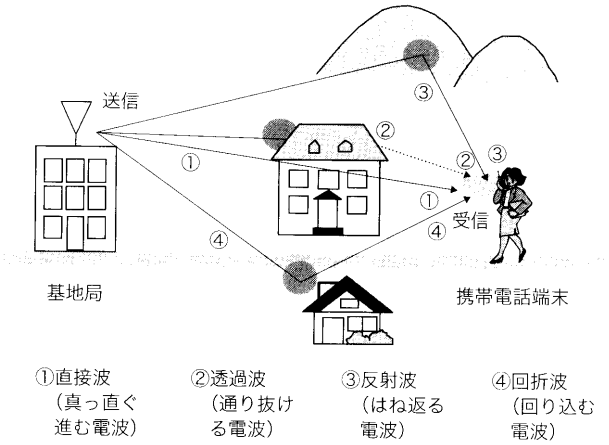


図 6.13　移動通信の電波伝搬モデル

これらの複数の電
波が携帯電話端末へ届くと，直接波はもっとも早く受信点に到来するのに対し，遠方の山やビル壁面で反身ける反射波は伝わる距離が良くなるので，直接波に比較し，時間的に遅れて受信点に到達する．各電波は，山（電波強度が強い）と谷（電波強度が弱い）がある波形であるので，これら複数の電波が前なり合うことによって，電波の干渉が起こり，電波の波形は時間とともに複雑こ変化する．この規象を**マルチパスフェージング**とよぶ．

・・・どうやって解決している？

知識創造理論において，知識を「暗黙知」と「形式知」に分け，その変換プロセスを示した **SECI モデル**では，知識変換の活動を凶 7.1 に示す以下の 4 つのステップで表現している．

・共同化（Socialization）：共体験などによって暗黙知を獲得・伝達する
・表出化（Externalization）：暗黙知を共有できるよう形式知に変換する
・連結化（Combination）：形式知を組み合せて形式知を創造する
・内面化（Internalization）：形式知をもとに個人が実践を行い体得する

ここで，暗黙知は言葉や文章で表すことの難しい主観的で身体的な知識のことをいう．具体的には，想い，視点，メンタルモデル，熟練，ノウハウなどが

あげられる．一方，形式知は，言葉や文章で表現できる客観的で理性的な知識のことで，コンピュータネットワークやデータベースを活用して容易に組換えや蓄積が行えるものである．

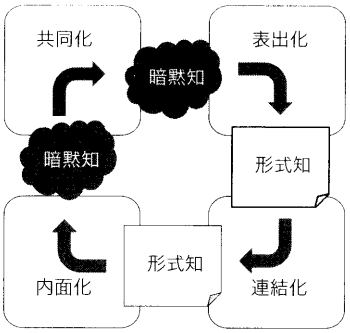


図 7.1　SECI モデル

従来の産業型社会は 100 人集まれば，一人の 100 倍の力を発揮できる社会であった．サイバー社会は**数人の非常に傑出したメンバからなるグループが，数万人の組織を凌駕する**働きをする可能性を秘めた社会である．

クラウドコンピューティング（Cloud Computing）は，サーバ側の処理能力を向上させる**負荷分散技術**と，コンピュータ資源を有効に利活用する仮想化技術によって実現されている．さらに，ビジネス的な観点からは，これまで主流だったオンプレミス（On－premise）とよばれるサーバの社内設置と自社運から，それらを業務委託するアウトソーシング（Outsourcing）への変化とえることができる．業務委託の形態は，以下のとおり分類できる．

・ハウジング（Housing Service）：自社所有のサーバを回線設備の整った専門業者の施設に設置する形態
・ホスティング（Hosting Service）：専門業者が提供する物理的なサーバを利用する形態
・IaaS（Infrastructure as a Service）：専門業者から仮想的なサーバ，CPU，ストレージなどのインフラをサービスとして受ける形態
・PaaS（Platform as a Service）：専門業者からアプリケーションを稼働させるための仮想的な基盤（プラットフォーム）をサービスとして受ける形態
・SaaS（Software as a Service）：専門業者からアプリケーション（ソフトウエア）をサービスとして受ける形態

上記の分類で，IaaS，PaaS，SaaS は，**XaaS** とよばれ，仮想化技術によっコンピュータ資源を有効に利活用して，コストを低廉化しているクラウドコピューティングである．

XaaS ザース

危殆化（きたいか）

＝＝＝Web＝＝＝
危殆化とは、「危険な状態になること」「危うくなること」を意味する語である。コンピュータの性能向上によって暗号化技術をはじめとするセキュリティ技術の安全性が、相対的に低下していくこと指すことが多い。
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

陸・海・空・宇宙空間に次ぐ 5 番目の社会
錦城として「サイバー空間」が米国政府により 2011 年に定義された．**サイバー空間**は，ICT を用いで情報をやりとりするインターネットを中核とした仮想的領域のことである．この概念の背景には，従来の四つの領域と同じくサイバー空間も，国際政治，国際公共財（Global Commons）などで扱うものとして捉えられていることがある．

DMZ
　インターネットに公開する Web サーバやメールサーバを運用する場合は，外部からこれらにアクセスできるようにしなければならない．そこでファイアウォールの外に，外部からアクセス可能な **DMZ**（DeMilitarized Zone：非武装地帯）とよばれるゾーンを設け，ここに外部からアクセスを許可する Web サーバやメールサーバを置いている．DMZ は非武装地帯を意味する軍事用語であり，外部公開用のゾーンが果たす役割から命名されている．このとき DMZ と外部との間にもファイアウォールを設け，公開しているサービス以外のパケットを受け付けないようにする．

（1）共通鍵暗号方式

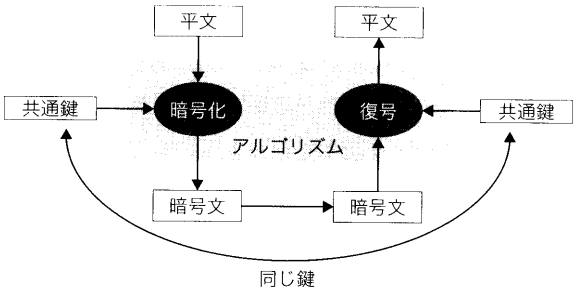


図 9.6　共通鍵暗号方式

図 9・7 に示すように，「ひらがな（あいうえお…）の各文字を 3 文字後ろにずらす」がある．ここで，「後ろにずらす」がアルゴリズムで，3 文字が鍵である．この暗号アルゴリズムは，シーザー暗号ともよばれ，紀元前 1 世紀には使用されていた

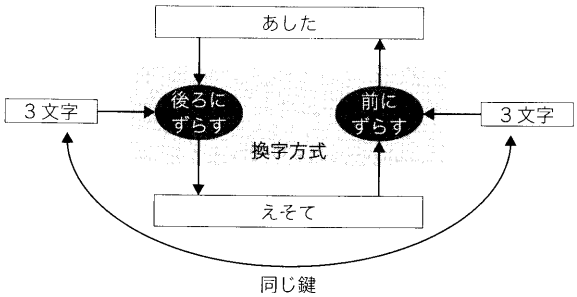


図 9.7　共通鍵暗号方式の例

（2）公開鍵暗号方式

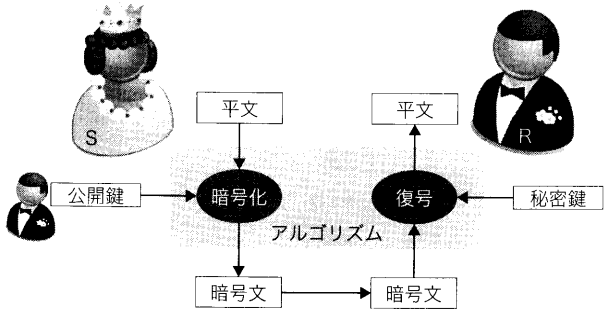


図 9.9　公開鍵暗号方式

図 9.9 に示すように，送信者 S は受信者 R の公開鍵を使用して平文を暗号化して送信し，受信者 R は受信した暗号文を自らの秘密鍵を使用して復号する．ここでは，公開鍵と対になっている秘密鍵を使用しないと復号できないことがポイントであり，その秘密鍵をもつ人だけが復号可能である．したがって，公開鍵は，盗聴者に知られてもかまわない．

本人認証としては，9．1 節で紹介したパスワードなど本人しか知らない情報（**WYK**：What You Know）を入力させる知識認証，トークン（ワンタイムパスワード），IC カードなどの所持（**WYH**：What You Have）による物理認証，指紋，虹彩，手のひら静脈など，本人の特徴（**WYA**：What You Are）で識別する生体認証がある．

セキュリティプロトコルは，インターネット上の通信において，盗聴，改ざん，なりすましなどの不正な行為からデータを保護する仕組みが施されたプロトコルである．Web 通信を暗号化する **SSL**（Secure Socket Layer），メールを暗号化する S/MIME（Secure Multipurpose Internet Mail Extensions），2 地点間通信を暗号化する IPsec（Security Architecture for Internet Protocol）などが代表例である．いずれのセキュリティプロトコルも，最初に公開鍵暗号方式で共通鍵を送り，以降は共通鍵で暗号化／復号を行うハイブリット暗号方式を用いている．

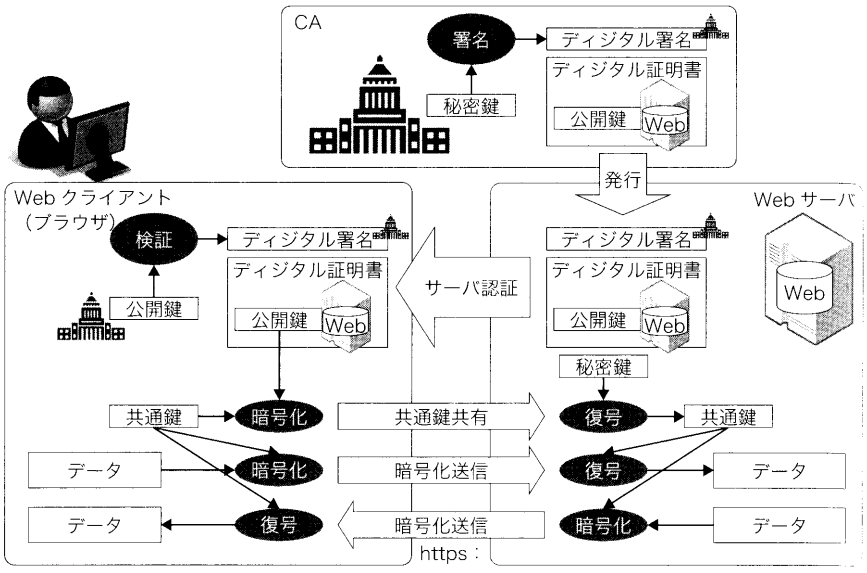


図 9.16　SSL/TLS プロトコル

マルウェア（Malware）は，Malicious Software（悪意のあるソフトウェア）を短縮した造語であり，コンピュータウィルス，スパイウェア，ポットなどの不正プログラムの総称である．

（1）コンピュータウィルス
　コンピュータウィルス（Computer Virus）は，ほかのファイルやプログラムに寄生して悪事をはたらくソフトウェアである．

2）スパイウェア
　スパイウェア（Spyware）は，利用者や管理者の意図に反してインストールされ，ユーザの個人情報やアクセス履歴などの情報を収集する不正プログラムである．

3）ボット
　ボット（Bot）は，感染したパソコンをインターネット経由で外部から操る目的をもつ不正プログラムである．